**ATTACHMENT A**

**LOCATION TO BE SEARCHED**

The residence located at 53 N. Center Street, Redlands, California, 92373 including all rooms, attics, basements, and other parts therein, garages, vehicles, or parking spaces associated with the property, storage rooms, trash containers, safes, and any out buildings of any kinds located thereon (hereinafter "SUBJECT LOCATION"). The SUBJECT LOCATION is further described as a two-story unit in a multi-unit complex with light brown stucco and dark brown wood paneling. The numbers "53" are affixed to the residence above the walkway near the front entrance of the door, are dark colored with a light background, and are approximately three inches in height. The door frame is dark brown in color and on the ground floor. A window approximately two by one foot is located on the left wall on the entry way to the door. The door faces to the east. Approximately three feet to the right of the front door is a four foot by three foot bay window.

The SUBJECT LOCATION includes a two-car detached garage with light brown stucco and dark brown trim. The garage is part of a four garage door detached structure directly behind the residence. The garage door faces to the west.

**ATTACHMENT A-2**

**PROPERTY TO BE SEARCHED**

Black Lexus IS300 California license plate #5KGD203, handicap placard 360466F, vehicle identification number JTHBD192X50094434.

**ATTACHMENT B**

**I. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of (1) 18 U.S.C. § 844(d) (Transportation or Receipt of Explosive Devices with the Intent to Injure or Kill); (2) 18 U.S.C. § 844(i) (Attempted Destruction by Explosives of Any Building, Person, or Property); and (3) 18 U.S.C. § 844(n) (Conspiracy):

a. Explosives, smokeless powder, black powder, gunpowder, or any other item that can be pipes, and wires;

b. Pipes and any items that may cause fragmentation;

c. Initiating devices to include burning fuse, hobby fuse, blasting caps, manual or electrical timers, dry cell batteries, electrical wire, alligator clips, electrical tape of assorted colors commonly used to secure exposed electrical wiring;

d. Books related to the construction of explosives;

e. Tools used in the construction of explosives such as include hand held vise grips, table mounted vise grips, pipe cutters, electrical; and non-electrical drills and drill bits.

f. Address and/or telephone books, telephones, pagers, answering machines, customer lists, and any papers reflecting names, addresses, telephone numbers, pager numbers,

fax numbers and/or identification numbers of sources of supply of explosives;

g. No more than 5 documents and records, including electronic mail and electronic messages, reflecting the ownership, occupancy, possession, or control of the SUBJECT LOCATION, including lease/rental agreements, rent receipts, registration documents, bank records, utility bills, telephone bills, other addressed envelopes, and correspondence;

h. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

i. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at

that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the

conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

7. The government is allowed to share the information obtained from this search (to include copies of digital media) with any government agency investigating, or aiding in the investigation of, this case or related matters.